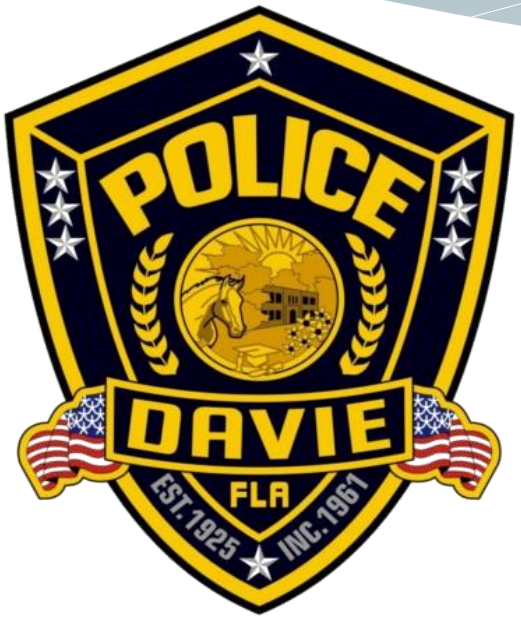
DAVIE POLICE DEPARTMENT



Sergeant Rob Choquette
Economic Crimes Unit

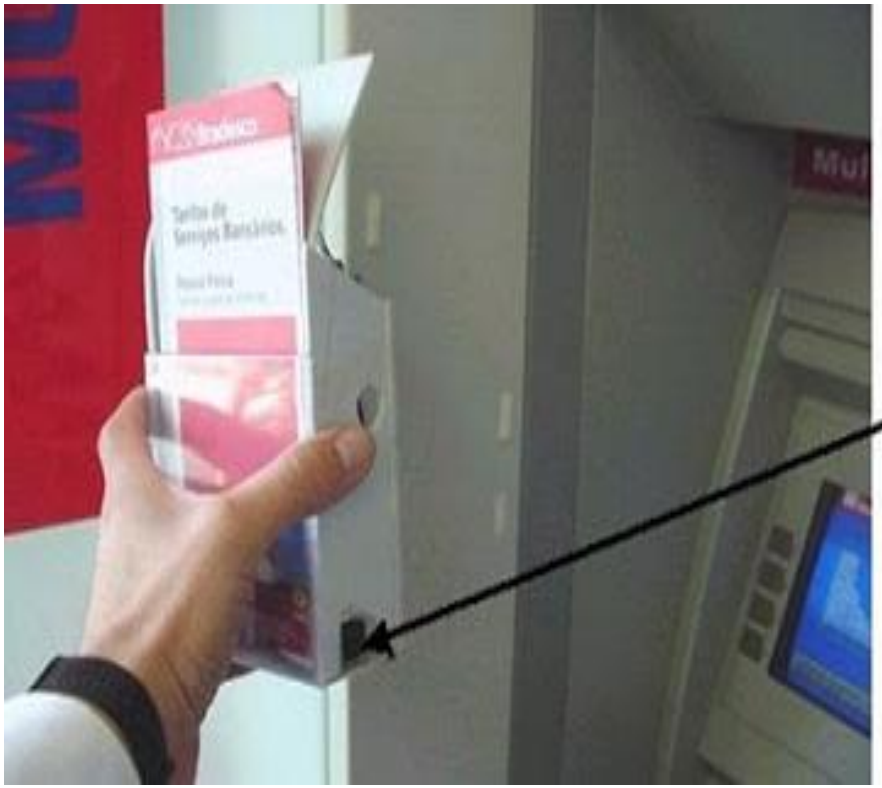
FRAUD

Wrongful or criminal deception intended to result in financial or personal gain.

Common Fraud Schemes

- Credit Card (CC) Fraud
  - CC numbers are obtained by various means such as:
    - Access/skimming devices:
      - These are purchased via the Internet on illegal websites. CC info can be accessed by employees such as bank employees, medical facility employees, even government employees, phishing emails, computer hacking, applications, and data breaches.
    - Plastic cards with magnetic strips can be re-encoded with compromised CC numbers and personal information.
      - If suspect(s) are unable to re-encode magnetic strip, the CC numbers can be embossed on a plastic card, usually with a bank emblem on it. CC must then be manually entered, which many businesses will not do. This method is not as common anymore, but it still happens.
    - CC number is used to make purchases via the Internet

Common Fraud Schemes

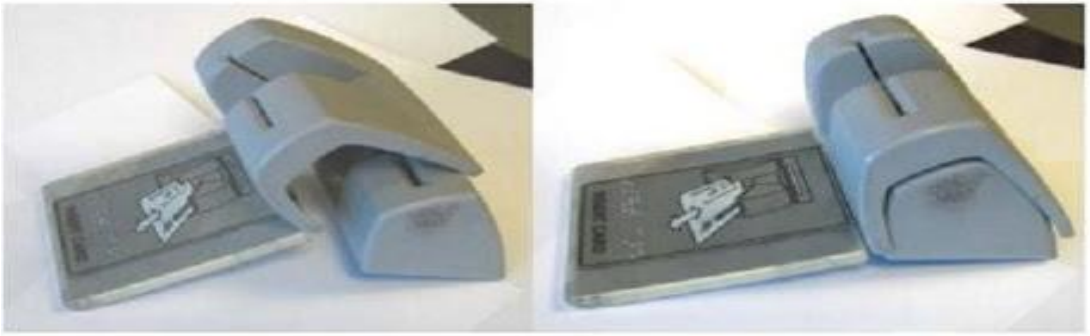


There is a camera concealed behind the glass window in the base of the leaflet box. It photographs PIN codes entered by users at the ATM.

Common Fraud Schemes

Original ATM card slot

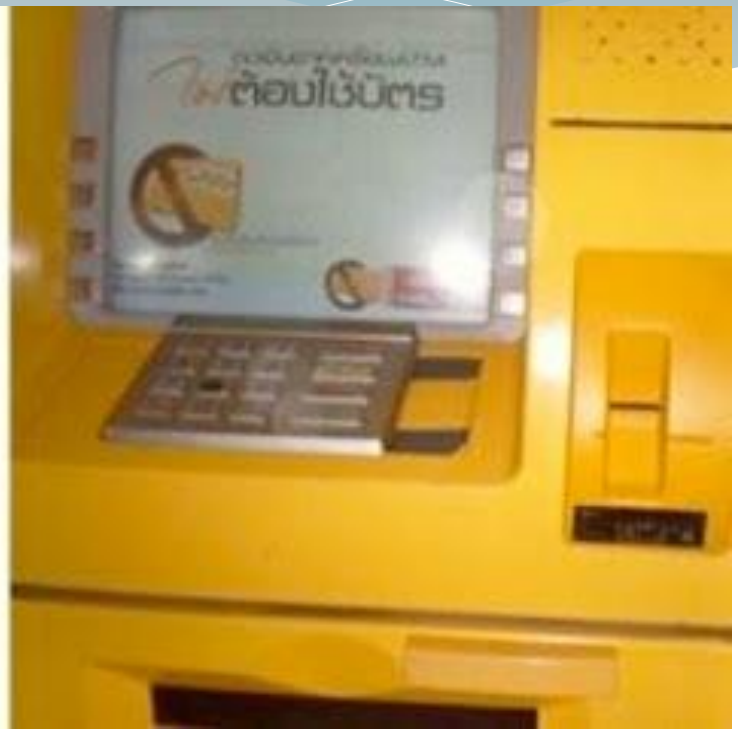
Card skimming device



Card skimming device fitted over ATM card slot

Common Fraud Schemes

Fake keyboard to Capture PIN Codes



Card skimming device

Both devices are used together to capture users' account access information.

Common Fraud Schemes

- Personal Information is used to apply for a CC, phone service, loans, or to take over personal accounts, etc.
  - Personal Information generally includes any or all of the following:
    - name,
    - Address
    - date of birth
    - social security number
    - DL number
    - Any identifier assigned to an individual.

Account Takeover

- Occurs when an unauthorized subject (may or may not be a suspect) is added to the account via the internet or telephone.
  - Information such as account phone number and address, usually a "drop" address, may be changed on the account.
  - Savings and other accounts at the same bank that may or may not be linked are compromised and the money is transferred into the initial compromised account.
  - A new debit card or checkbook assigned to the unauthorized subject is obtained, mainly by being mailed to the drop address.
  - ATM withdrawals and/or purchases are made with the new debit card until account is wiped out or the fraud is caught.
  - Money orders may be purchased due to daily withdrawal limits at ATM.

Account Takeover Cont....

- Access to account balance, check sequence number, transactions and copies of checks, which shows your signature, from bank account can be accessed through Online Banking.
- Checks can be counterfeited and signature forged.
- Counterfeit checks are then made payable to a "mule" who enters a bank or check cashing store to cash the check.
- Suspects are usually waiting outside for the mule to walk out with the money. If the suspect(s) see law enforcement arriving, they quickly leave, leaving the mule behind to get arrested.

How to Prevent Becoming a Victim

- Do **NOT** open emails that contain links you are not familiar with. Even if they come from a known contact, sometimes their email account was hacked.
- Use a Credit Card instead of a debit card whenever possible.
- Be careful when providing your personal information on applications, including doctor office visits.
- Do **NOT** use the same password for all of your accounts.
- When possible, have your savings account at a bank different from checking or debit accounts.
- Monitor your credit report regularly.
- Do **NOT** provide personal information over the phone when contacted by any business unless you are **100%** sure of who you are speaking to. You can always look up the number of the company and call them back yourself to verify. Do **NOT** believe the contact info they give you.
- **File your income taxes as early as possible.**

Craigslist Scams

You can thwart would-be scammers by following the rules below

- **DEAL LOCALLY WITH PEOPLE YOU CAN MEET IN PERSON** - follow this one rule and avoid 99% of scam attempts.
- **NEVER WIRE FUNDS VIA WESTERN UNION, MONEYGRAM or other wire service** - anyone who asks you to do so is likely a scammer.
- **FAKE CASHIER CHECKS & MONEY ORDERS ARE COMMON** -Banks will hold you responsible when the fake is discovered weeks later.
- **CRAIGSLIST IS NOT INVOLVED IN ANY TRANSACTION**, and does not handle payments, provide escrow, "buyer protection" or "seller certification."
- **NEVER GIVE OUT FINANCIAL INFORMATION** (bank account number, social security number, eBay/PayPal info, etc.).
- **AVOID DEALS INVOLVING SHIPPING OR ESCROW SERVICES** and know that **ONLY A SCAMMER WILL "GUARANTEE" YOUR TRANSACTION**.
- **DO NOT RENT HOUSING OR PURCHASE GOODS SIGHT-UNSEEN** -that amazing rental or cheap item may not exist.
- **DO NOT SUBMIT TO CREDIT OR BACKGROUND CHECKS** until you have met the job interviewer or landlord/agent in person.

What to do if you are a Victim

- Immediately report the fraud to your banking institution and/or CC company.
- Check your credit report.
- Place a Fraud Alert on with all three credit reporting agencies.
- File a police report with the proper jurisdiction. If jurisdiction cannot be determined, file a police report in the jurisdiction you reside in.
- Fill out and return any forms or affidavits in a timely manner.
- Tax fraud- contact the IRS and visit their website for the proper forms requiring completion.